ความปลอดภัยบนโลกออนไลน์

ดร.ชาลี วรกุลพิพัฒน์
CISSP, CISA
หัวหน้าห้องปฏิบัติการวิจัยความมั่นคงปลอดภัยไซเบอร์ (CSL)
หน่วยวิจัยไร้สาย ข้อมูลความมั่นคงและนวัตกรรมอิเล็กทรอนิกส์ เพื่ออนุรักษ์พลังงานและสิ่งแวดล้อม (WISRU)
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
Chalee.vorakulpipat@nectec.or.th

ประวัติวิทยากร

ดร.ชาลี วรกุลพิพัฒน์

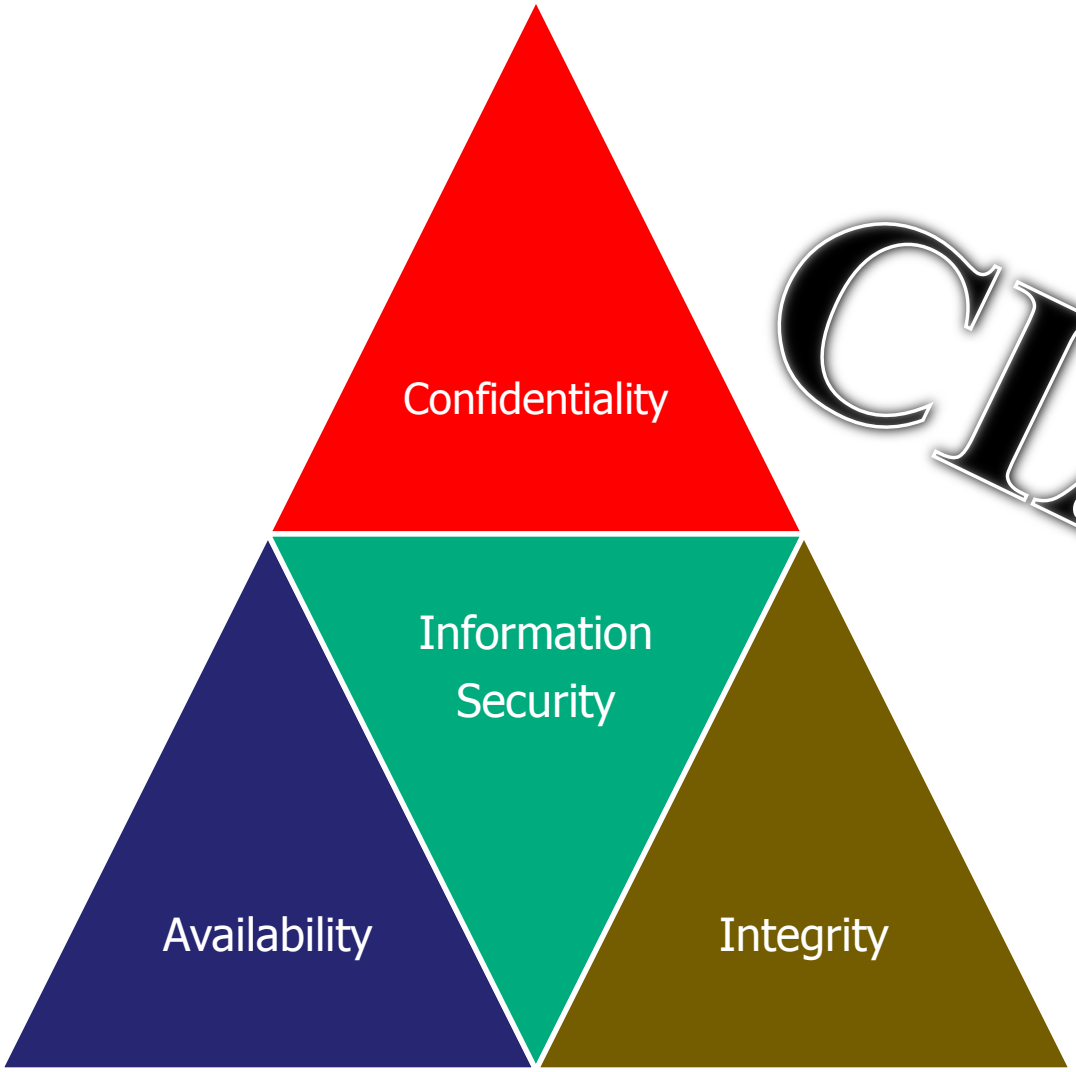
- ประวัติการศึกษา
  - PhD (Information Systems) University of Salford ประเทศอังกฤษ
  - วท.ม. (เทคโนโลยีสารสนเทศ) มหาวิทยาลัยเกษตรศาสตร์
  - วศ.บ. (อิเล็กทรอนิกส์) สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
- ประวัติการทำงาน
  - หัวหน้าห้องปฏิบัติการความมั่นคงปลอดภัยไซเบอร์

    ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) (2540-ปัจจุบัน)
  - อนุกรรมการและเลขานุการ คณะอนุกรรมการมั่นคงปลอดภัย ภายใต้คณะกรรมการธุรกรรมอิเล็กทรอนิกส์ (2552-ปัจจุบัน)
  - หัวหน้า ThaiCERT (2553-2554)
  - อาจารย์พิเศษ (เกษตรศาสตร์, ศรีปทุม, ธุรกิจบัณฑิตย์, พระนครเหนือ)
  - วิทยากรบรรยายพิเศษให้หน่วยงานภาครัฐและเอกชน

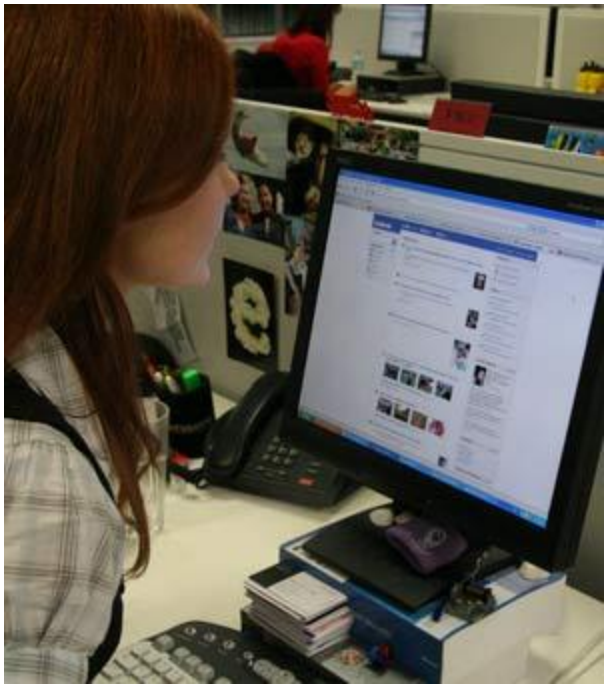
ประวัติวิทยากร

- Certificate: CISSP, CISA, IRCA ISMS Lead Auditor ISO/IEC 27001
- รางวัลและเกียรติยศ
  - NECTEC Star 3 ครั้ง (2553,2555,2556)
  - รางวัลแนวคิดวิจัยและพัฒนา (ชมเชย) กสท โทรคมนาคม ในงานวิจัย Green Email: อีเมล์ไร้สแปม 2554
  - รางวัลวิทยานิพนธ์ดีเยี่ยม (ชนะเลิศ) สาขาเทคโนโลยีสารสนเทศและนิเทศศาสตร์ สภาวิจัยแห่งชาติ 2552
  - Outstanding Paper Award (Highly Commended), Journal of Knowledge Management 2552
  - Featured Student, Informatics Research Institute, University of Salford 2549
  - ทุน ก.พ. (กระทรวงวิทย์) ศึกษาต่อในระดับปริญญาเอก 2547
- บทความวิชาการ ต่างประเทศ 23 บทความ ในประเทศ 7 บทความ
- แต่งหนังสือ “UML ภาษามาตรฐานเพื่อผู้พัฒนาซอฟต์แวร์” ซีเอ็ดยูเคชัน

CIA ของหน่วยงาน



ทำไมต้องคำนึงถึง security



Facebook as a Diary

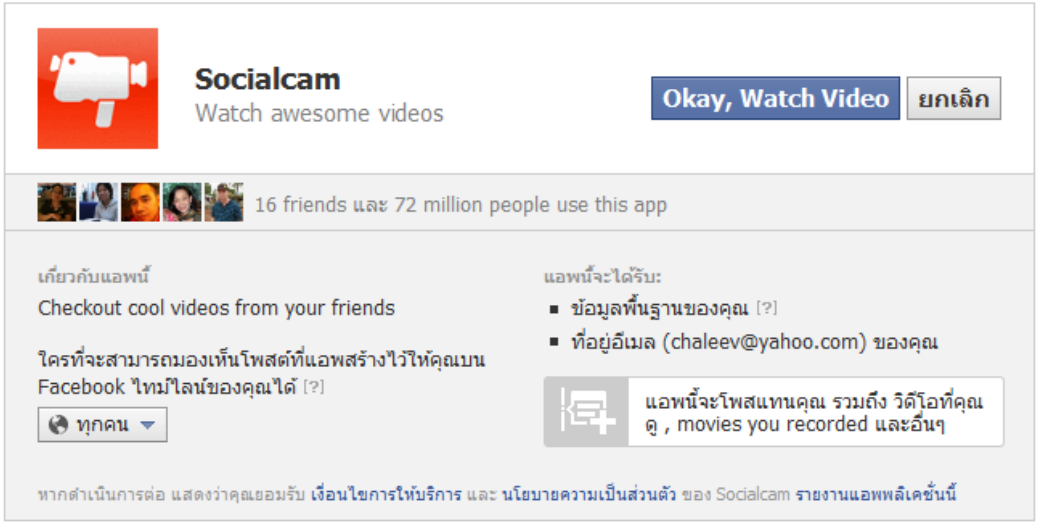
- บอกว่าเราทำอะไร อยู่ที่ไหน
- การโพสต์ข้อความเชิญชวนให้ขโมยเข้าบ้าน

Facebook as a Data Storage

- ข้อมูลที่โพสต์ลงบนอินเตอร์เน็ต อาจถูกเก็บอยู่ในนั้นได้เป็นสิบๆ ปี อาจเป็นหลักฐานทางกฎหมายได้

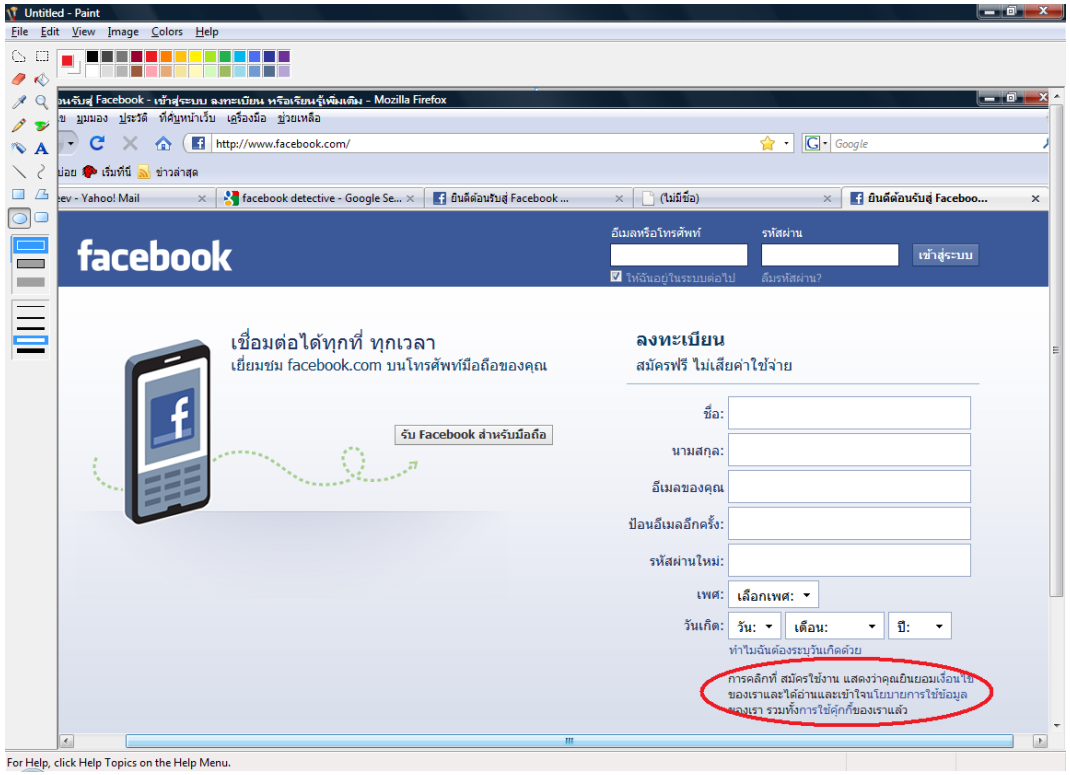
Facebook knows what we are DOing

- เรากำลังดูข้อมูลอะไร คนอื่นทราบหมด
- *"The more function an application has, the less secure it tends to be,"* **Roger Thompson, chief research officer for AVG**



Terms & Conditions

- เราเคยได้อ่านหรือเปล่า
- หรือเราโกหกว่าอ่านแล้ว
- **BIG LIAR!!!!**

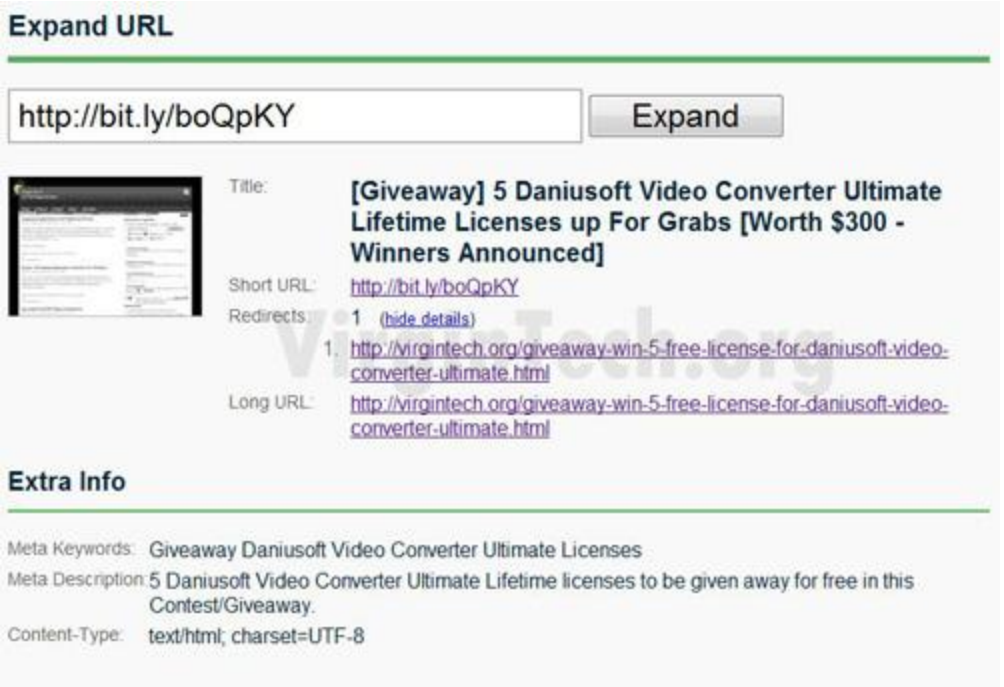


Spam Hoax

- Spam Hoax ผ่านกลุ่มต่างๆ ใน Social Network
- ข้อมูลใน Facebook ถูกส่งผ่านเร็วกว่าสื่ออื่นๆ
- การ Unsubscribe Spam ประโยชน์หรือโทษ???

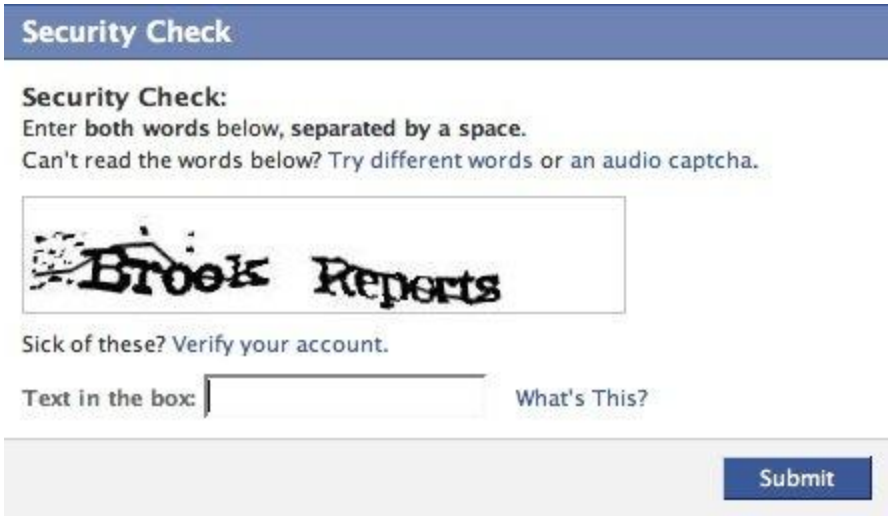
Phishing/Virus/Malware thru Facebook

- หลายคนรู้จักวิธีหลีกเลี่ยง Phishing/Virus/Malware เป็นอย่างดี แต่ตกเหยื่อด้วยวิธี Short URL (เช่น bit.ly) ผ่าน Facebook
- แก้ด้วยวิธี Preview



CAPTCHA

- **Facebook อาจให้ผู้ที่โพสต์ URL link ไปยัง Wall ของคนอื่นต้องตอบคำถาม CAPTCHA ก่อน เพื่อมั่นใจว่าผู้ส่งไม่ใช่ Machine Spammer**
- **Re-CAPTCHA???**



การป้องกัน

- **Balance**
  - **Technical vs Non-Technical Issues**
  - **Security vs Ease of Use or Convenience**
- **ท่านจะทำอย่างไร ถ้าวันหนึ่งผู้บริหารของท่านสั่งห้ามใช้ Facebook หรือ Youtube**

ไม่เปิดเผยข้อมูลส่วนตัว

- เมื่อกรอกข้อมูลส่วนตัวลงพวก Facebook เราต้องทราบก่อนว่าผู้ใดจะสามารถเห็นได้บ้าง เฉพาะเพื่อน เพื่อนของเพื่อน หรือใครก็ได้
- ในยุค Web 2.0 Hacker สามารถขโมยข้อมูลเพื่อนำไปขายหรือใช้ประโยชน์ทางธุรกิจได้

สงสัยไว้ก่อน

- อย่าเชื่อข้อมูลใน Social Network จนเกินไป ควรจะสงสัยไว้ก่อนว่าข้อมูลนั้นน่าเชื่อถือ มีประโยชน์หรือไม่

ระวังก่อนพิมพ์

- ทุกอย่างที่คุณพิมพ์ลงไป อาจย้อนกลับเข้ามาหาตัวคุณได้ โดยเฉพาะการโชว์พฤติกรรมที่ไม่ค่อยดีลงไป

ทำตัวเหมือนฝ่ายบุคคล

- หากคุณกำลังติดต่อกับคนแปลกหน้าผ่าน **Social Network** คุณต้องทราบให้ได้ก่อนว่าคนๆ นั้นที่แท้จริงคือใคร เหมือนใช้ระบบสกรีนคนตอนสมัครงาน

ระวังเป็นพิเศษตอน On the Move

- หากกำลังใช้ Social Network บนโทรศัพท์มือถือ จะเพิ่มความเสี่ยง
- คำนึงเรื่อง Location-based Service
- สมบัติล้ำค่า 3 อย่างอาจถูกขโมยในเวลาเดียวกัน –
  - โทรศัพท์มือถือ
  - ข้อมูลข้างใน
  - ตัวตน

กลับไปอ่าน Terms & Conditions

- หากยังมีข้อสงสัย ให้กลับไปอ่าน Terms & Conditions ให้ดี โดยเฉพาะ Privacy Policy
- หากไม่เห็นด้วย ก็ไม่ควรใช้

กรณีศึกษา

จำกัดการเข้าถึง

- ใน USA และ UK ตามสถาบันการศึกษาหรือห้องสมุดพยายามที่จะจำกัดการใช้งาน เนื่องจาก MySpace กลายเป็น “such a heaven for student gossip and malicious comments” และ MySpace ใช้ internet bandwidth กว่า 40% ในหนึ่งวันในการใช้เว็บ ทำให้ internet ช้าลง

ปัญหาเรื่อง Profile

- สร้างความเสียหายแก่นักเรียนเอง: มีรายงานว่าใน USA นักเรียนส่วนใหญ่มักใส่ profile ที่ดูสูงหรือดู over เกินไป ลงใน MySpace ของตนเอง นายจ้างอาจไม่พิจารณาบุคคลแบบนี้

การจำกัดอายุ >= 14 ปี

- คนที่อายุ 14-15 จะถูกกำหนด profile ให้เป็น private
- 16 หรือมากกว่า จะให้เลือกสิทธิในการเข้าถึงได้
- เด็กจะถูกจำกัดการเข้าถึงข้อมูลที่ไม่เหมาะสม เช่น sex contents
- ในปี 2006 เด็กวัยรุ่นหญิงฆ่าตัวตาย อันเนื่องมาจากการถูกกลั่นแกล้งและใส่ความจากเพื่อนวัยรุ่นชายคนหนึ่งใน MySpace ซึ่งแท้จริงแล้ววัยรุ่นชายคนนั้นไม่มีตัวตนจริง แต่เป็นการปลอมตัวโดยแม่ของเพื่อนของเหยื่อ
  - http://www.foxnews.com/story/0,2933,312018,00.html
  - http://en.wikipedia.org/wiki/Suicide_of_Megan_Meier

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact Wikipedia

Toolbox

Print/export

Languages
Español
Italiano
Português

Suicide of Megan Meier

From Wikipedia, the free encyclopedia

Megan Taylor Meier (November 6, 1992 – October 17, 2006) was an American teenager from Dardenne Prairie, Missouri, who committed suicide by hanging three weeks before her fourteenth birthday. A year later, Meier's parents prompted an investigation into the matter and her suicide was attributed to cyber-bullying through the social networking website MySpace. The mother of a friend of Meier, Lori Drew, was later indicted on the matter in 2008, but in 2009, Drew was acquitted.[1]

Contents [hide]

Background [edit]

Megan Meier was born in O'Fallon, Missouri, to Christina "Tina" Meier and Ronald Meier. She had lived in nearby Dardenne Prairie during her childhood, with her parents and sister Allison.

From the third grade, Megan had been under the care of a psychiatrist. She had been prescribed citalopram, methylphenidate and

Megan Meier

Megan Meier

Born	Megan Taylor Meier November 6, 1992 O'Fallon, Missouri, U.S.
Died	October 17, 2006 (aged 13) Dardenne Prairie, Missouri, U.S.
Cause of death	Suicide by hanging
Resting place	Saint Charles Memorial Gardens

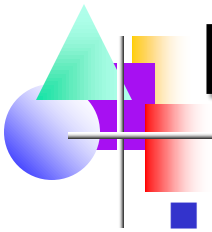
ประเด็นอื่นๆ ในกรณีศึกษา

- ลิขสิทธิ์เพลง สังคม วัฒนธรรม กฎหมาย
- Google ขอใส่ช่อง search ลงในเว็บ MySpace ซึ่ง MySpace จะได้ประโยชน์หรือเสียผลประโยชน์?

กรณีศึกษา: Security Failure

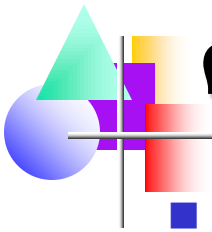
ASSOCIATED PRESS

Olatunji Oluwatosin, a Nigerian national accused of stealing personal information from people through bogus accounts with ChoicePoint Inc., pleaded no contest last week in Los Angeles Superior Court. The company disclosed yesterday how many people in each state may have been victimized.



Hacker

- **White-hat hackers**
  - มีจรรยาบรรณ ตรวจสอบระบบเพื่อหาช่องโหว่ เพื่อจะได้แก้ไข
- **Black-hat hackers**
  - เป็น cracker ที่ทำลาย ก่อปัญหา

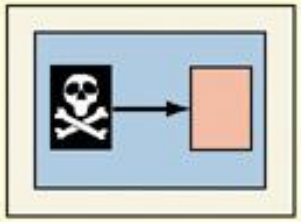


ตัวอย่างการภัยคุกคาม

- Virus
- Worm
- Spyware
- DoS
- Phishing
- Botnet
- Spam

ไวรัสคอมพิวเตอร์ทำงานอย่างไร

Just as a biological virus disrupts living cells to cause disease, a computer virus—introduced maliciously—invades the inner workings of computers and disrupts normal operations of the machines.



1 A virus starts when a programmer writes a program that embeds itself in a host program.

2 The virus attaches itself and travels anywhere that the host program or piece of data travels, whether on floppy disk, local area networks, or bulletin boards.

3 The virus is set off by either a time limit or some set of circumstances, possibly a simple sequence of computer operations by the user (e.g., open an attachment). Then it does whatever the virus programmer intended, whether it is to print "Have a nice day" or erase data.

Phishing

Account Information - Message (HTML)

File Edit View Insert Format Tools Actions Help

Reply Reply to All Forward

From: HSW Bank.com Sent: Fri 11/25/2005 2:04 PM
To: John Doe
Cc:
Subject: Account Information

howstuffworks

Dear customer:

During an automated audit on 11/20/2005, we discovered discrepancies in your account. Please follow the link below to confirm your account information with us. Failure to respond within five business days will result in the termination of your account.

Sincerely, HSW Bank

http://hswbank.accountmaintenance.com/verify/0984325.htm)

Remember, Old National will never send you emails asking for your personal and/or financial information.

From: ID-protection@Oldnationalbank.com
Date: 8/5/2005 2:57 PM
Subject: Important Account Information (Unusual login attempts - Case ID:1234567)

Dear Old National Bank Customer,

We recently noticed several attempts to log in to your personal account from a foreign IP address and we have reason to believe that your account was used by a third party without your authorization. If you recently accessed your account while traveling, the unusual login attempts may have been initiated by you.

The login attempt was made from:
IP address: 123.45.123.45
ISP Host: cache-66.proxy.aol.com

After three unsuccessful attempts to access your account, your personal Online Profile has been locked. This has been done to secure your accounts and to protect your private information. We are trying to make sure that your online transactions are secure.

This is not Old National's url

You must unlock your profile by going to:

http://www.Oldnationalbank.com/index.html

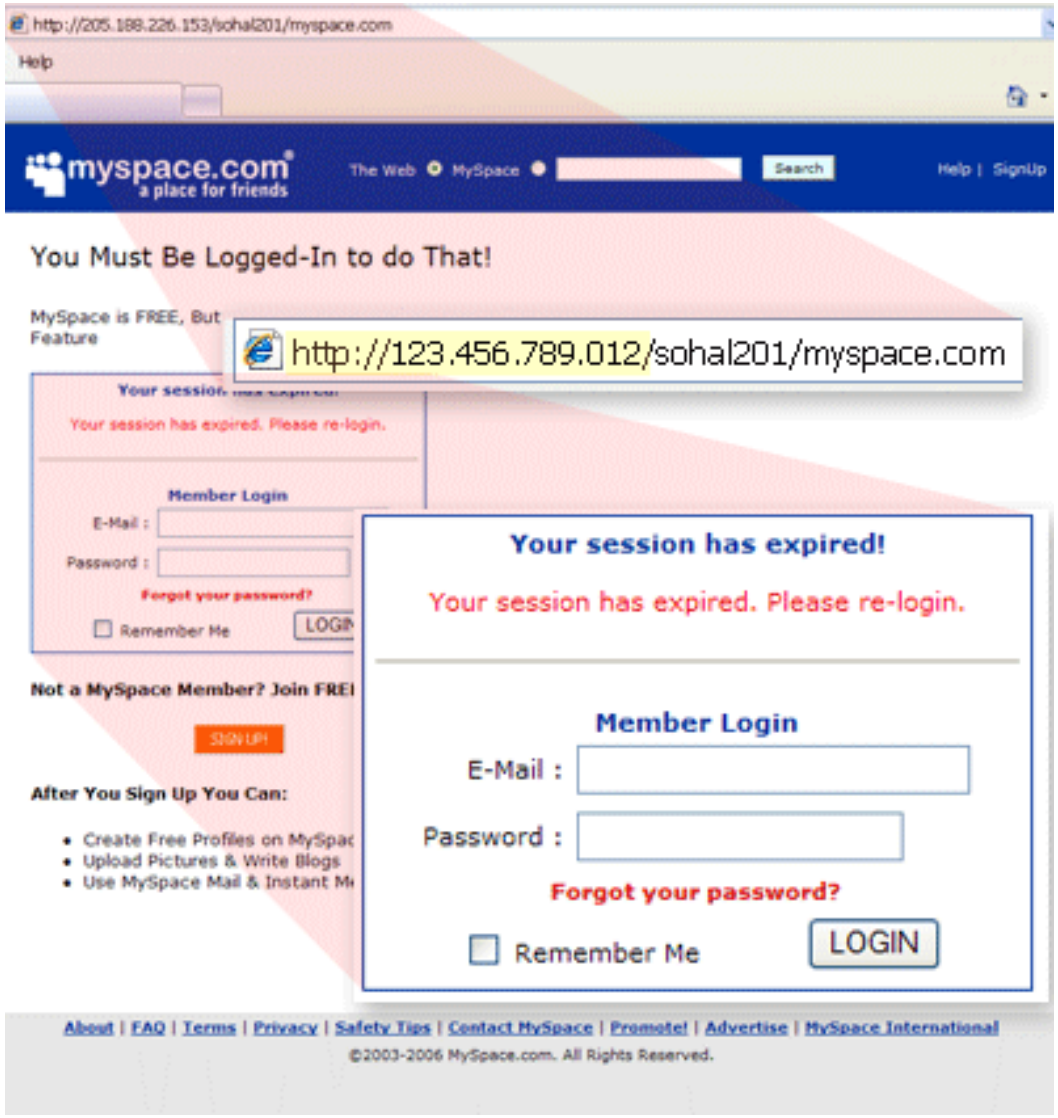
Be extremely cautious about clicking on links provided within emails.

If you should have any additional questions or concerns, please contact Customer Service at: service@Oldnationalbank.com

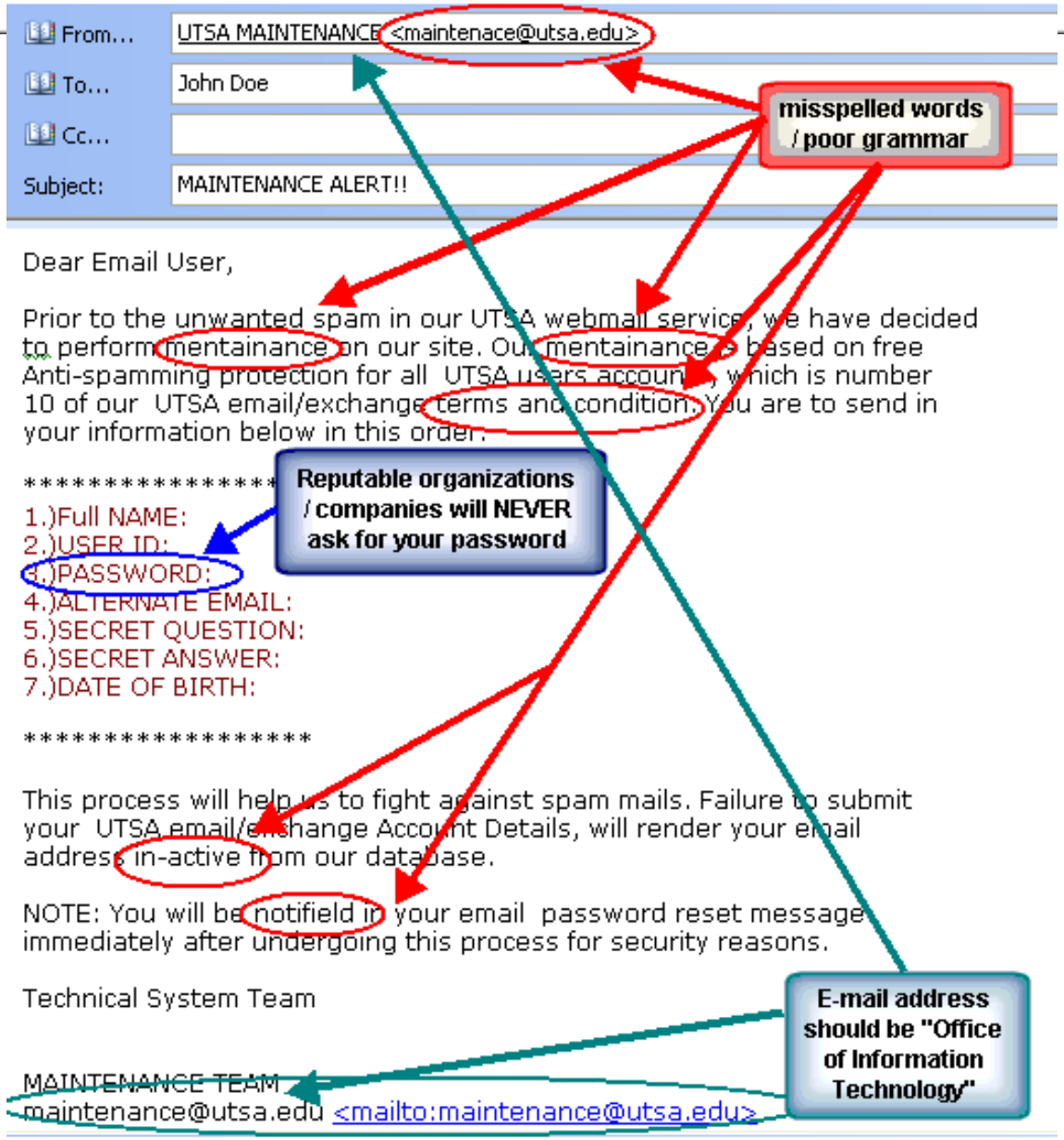
Thank you for using OldnationalBank ! 2005 Oldnationalbank Corporation. All rights reserved. Equal Opportunity Lender. Member FDIC.

Be wary of overall poor grammar & misspellings.

Phishing


http://205.188.226.153/sohal201/myspace.com
Help
myspace.com
a place for friends
The Web
MySpace
Search
Help | SignUp
You Must Be Logged-In to do That!
MySpace is FREE, But
Feature
http://123.456.789.012/sohal201/myspace.com
Your session has expired. Please re-login.
Member Login
E-Mail :
Password :
Forgot your password?
Remember Me
LOGIN
Not a MySpace Member? Join FREE
SIGN UP
After You Sign Up You Can:
Create Free Profiles on MySpace
Upload Pictures & Write Blogs
Use MySpace Mail & Instant Me
Your session has expired!
Your session has expired. Please re-login.
Member Login
E-Mail :
Password :
Forgot your password?
Remember Me
LOGIN
About | FAQ | Terms | Privacy | Safety Tips | Contact MySpace | Promote! | Advertise | MySpace International
©2003-2006 MySpace.com. All Rights Reserved.

Example of a typical, poorly-constructed phishing e-mail message



BotNet

ตัวอย่างการใช้ BotNet ในการส่ง spam mail

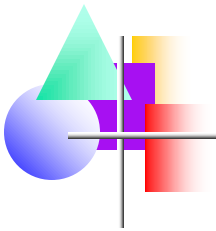
Source: http://en.wikipedia.org/wiki/Botnet

เราจะป้องกันอย่างไร?

- มีมาตรการป้องกันที่ดี เช่น มีระบบป้องกันไม่ให้คนที่ไม่มีสิทธิเข้าถึงข้อมูล (login/password)
- มีระบบตรวจจับการบุกรุก เช่น Anti-virus
- จำกัดความเสียหายให้น้อยลง เช่นมี fault-tolerant system เพื่อให้ระบบพอจะใช้งานได้ไปก่อน (degraded mode)
- หาวิธีทำให้ระบบกลับคืนสู่สภาพปกติ เช่นมีแผนที่จะแก้ไขปัญหาให้เร็วที่สุดในกรณีที่เกิดความเสียหายต่อระบบ ต้องพิจารณาระหว่าง replace กับ repair
- สร้างความตื่นตัว (awareness) เช่น ออกกฎนโยบาย หรือ มีการฝึกอบรม IT security

สรุปการใช้คอมพิวเตอร์ให้ปลอดภัย

- ใช้สามัญสำนึก (Common sense) แม้จะไม่รู้รายละเอียดของกฎหมาย หรือ ไม่รู้ว่ามีกฎหมายนั้นด้วยหรือไม่
- การบุกรุก โจมตี ถือว่าผิดกฎหมาย
- แม้ว่าไม่ทำอะไรเลยก็อาจผิดกฎหมายได้ เช่น ถ้าท่านมีหน้าที่ป้องกัน แต่ละเลย
- มีจริยธรรมไว้ก่อน
- ศึกษาอย่างต่อเนื่อง



ขอบคุณครับ